REMARKS

Claims 1-31 are pending in the present application. Claims 1, 3, 13, 18, 20 and 30 have been amended herewith. Reconsideration of the claims is respectfully requested.

I.   35 U.S.C. § 102, Anticipation

The Examiner rejected Claims 1-8, 13-25 and 30 under 35 U.S.C. § 102 as being anticipated by Touboul. This rejection is respectfully traversed.

Amended independent claim 1, reads as follows:

> 1.   A method in a data processing system for preventing exchange of viruses with a device, the method comprising:
> maintaining preexisting content for the device in a first location in the data processing system;
> placing new content associated with the device in a second location, *wherein the new content is an update to the preexisting content*;
> combining the preexisting content and the new content in a third location to form merged content;
> performing a check for viruses on the merged content prior to performing a transfer of the new content; and
> storing the merged content as the preexisting content that is maintained in the data processing system if a virus is absent from the merged content.

As can be seen, Claim 1 recites the features of combining preexisting content and the new content in a third location to form merged content and performing a check for viruses on the merged content prior to performing a transfer of the new content. If a virus is absent from the merged content, the merged content is stored as the preexisting content on the data processing system, such that the data processing system maintains a current copy of the virus-free data that is sent to the device, and which is maintained on the data processing system as preexisting content. The step of combining preexisting content and the new content in a third location to form merged content is used to protect clients and servers from exchanging viruses via synchronization. The present invention recognizes that it is possible for a server to receive incremental updates that are infected with viruses that contain two or more parts, wherein the individual parts themselves are harmless. However, when the parts are compiled, the aggregate of the parts results in a virus. The following cited section in the Specification describes the basis for merging the

preexisting content and the new content in a third location to detect such aggregate viruses in the manner recited in claim 1:

> The present invention provides a method, apparatus, and computer implemented instructions for protecting clients and servers from exchanging viruses. The present invention recognizes that many clients, such as pervasive devices, communicate with servers via synchronization. This type of communication results in incremental updates to data or software being stored on a server for a client. With this situation, it is possible for a virus to contain two or more parts in which the individual parts are harmless. When all of the parts are put together, however, the aggregate results in a virus. With incremental updates, latent viruses, such as these, may be propagated to servers and other clients.
>
> The mechanism of the present invention eliminates these types of threats of introducing and spreading viruses. This mechanism is especially useful for clients that use a server as a primary means of communication. Updates or additions to data or software for a client are not sent to a client or stored on a server with existing data for the client until the union of this data is tested for the presence of a virus.

(Specification, page 12, line 17 to page 13, line 11). As is described above, the preexisting content and the new content are combined in a merge area (third location) on the server prior to transferring the updates to the client or storing the updates on the server. The merged content is analyzed to determine whether a virus is present in the combined or merged content. Only if a virus is absent does the merged content (i) get stored on the data processing system as preexisting content (Claim 1), or (ii) sent to the device (Claim 2). As a result, infected data, including aggregate viruses, may be detected and disinfected prior to that content reaching its destination.

The cited Touboul reference does not teach the feature of combining the preexisting content and the new content in a third location to form merged content, as expressly recited in Claim 1. Importantly, the new content is defined in Claim 1 to be an update to the preexisting content. In rejecting Claim 1, the Examiner equates Touboul's teaching of "a second DSP" as reading on the claimed "new content". Applicants urge that Touboul's "second DSP" is very different from the claimed "new content". As described by Touboul at column 3, line 66 – col. 4, line 19:

> The inspector 125 includes a content inspection engine 160 for examining a received
> Downloadable, e.g., the signed Downloadable 150 received from the developer 120, for generating a

Downloadable Security Profile (DSP) based on a rules base 165 for the Downloadable, and for attaching the DSP to the Downloadable. A DSP preferably includes a list of all potentially hostile or suspicious computer operations that may be attempted by the Downloadable, and may also include the respective arguments of these operations. Generating a DSP includes searching the Downloadable code for any pattern, which is undesirable or suggests that the code was written by a hacker. The content inspection engine 160 preferably performs a fall-content inspection. It will be appreciated that generating a DSP may also include comparing a Downloadable against Downloadables which Original Equipment Manufacturers (OEMs) know to be hostile. Downloadables which OEMs know to be non-hostile, and Downloadables previously examined by the content inspection engine 160. Accordingly, the rules base may include a list of operations and code patterns deemed suspicious, known hostile Downloadables, known viruses, etc.

As can be seen, the Downloadable Security Profile (DSP) is generated by an inspector based on rules for the Downloadable, and this DSP is then attached to the Downloadable. This DSP includes a list of potentially hostile or suspicious computer operations that may be attempted by the Downloadable. Importantly, this DSP is *not an update* for the Downloadable or for another DSP, and thus a "second DSP" as taught by the cited reference is not equivalent to the claimed "new content" as it is not an update to preexisting content (the preexisting content being equated by the Examiner to be the combination of the Downloadable and a first DSP). It is thus urged that Claim 1 is not anticipated by the cited reference, as every claimed element is not identically shown in a single reference.

Still further with respect to Claim 1, such claim has been amended to include features previously recited in Claim 3. As amended, Claim 1 recites "storing the merged content as the preexisting content that is maintained in the data processing system if a virus is absent from the merged content". In rejecting Claim 3 (whose features are now a part of amended Claim 1), the Examiner stated that the features of Claim 3 were taught by Touboul at col. 4, lines 35-38, col. 5, lines 48-58, col. 10, lines 14-18, and as shown in Figures 6 and 7. Applicants urge that these passages describe the download of a virus-scanned file *to a client device*. In contrast, the claimed storing step is with respect to storing the merged content in the data processing system itself (shown in the preferred embodiment in Figure 4, element 406). This is different from the claimed step recited in Claim 2, where the merged content is sent to the device (shown in the preferred embodiment in Figure 4, element 404). The claimed feature of storing the merged

content in the data processing system (as opposed to the client device) advantageously provides a new cache copy of the data in the data processing system, for use in subsequent update procedures by maintaining a copy of the information that is sent to the device. The cited reference does not teach such claimed feature, or its resulting advantages, and thus it is further urged that Claim 1 is not anticipated by the cited reference.

Applicants initially traverse the rejection of Claims 2-8 for similar reasons to those given above with respect to Claim 1.

Further with respect to Claim 3, Applicants urge that the cited reference does not teach the claimed feature of "wherein the data processing system receives the new content from the device". As described in the Specification at page 10 lines 27-30, page 11 lines 10-12, page 12 lines 2- 30 (with reference to Figure 5), updates (for which virus scanning is needed) may be received from the client device itself. The cited reference only contemplates receiving Downloadables from a developer (col. 3, lines 53-55), and checking these Downloadables before sending them on to an end-use device such as a client device. These teachings do not teach, suggest or otherwise contemplate receiving updates from the client device itself (see Figures 6 and 7 of Touboul, for example, where a developer certificate is attached, and subsequently authenticated). It is thus urged that Claim 3 is not anticipated by the cited reference, as every element of the claimed invention is not identically shown in a single reference.

With respect to Claims 13 (and dependent Claims 14-17), 18 (and dependent Claims 19-25) and 30, Applicants traverse for similar reasons to those given above with respect to Claim 1

Further with respect to Claim 20, Applicants traverse for similar reasons to the further reasons given above with respect to Claim 3.

Therefore, the rejection of Claims 1-8, 13-25 and 30 under 35 U.S.C. § 102 has been overcome.

II.   35 U.S.C. § 103, Obviousness

The Examiner rejected Claims 9-12, 26-29 and 31 under 35 U.S.C. § 103 as being unpatentable over Touboul et al., in view of Donahue (US Patent 6,202,207). This rejection is respectfully traversed.

A.   Initial Traversal of Claims 9 and 26

With respect to Claim 9 and 26, Applicants initially traverse for similar reasons to those given above with respect to Claim 1.

B.   Exclusion of US Patent 6,202,207

Further with respect to Claims 9 and 26, and initially with respect to Claims 10 (and dependent Claims 11 and 12), 27 (and dependent Claims 28 and 29) and 31, Applicants aver the following:

> The present application and US Patent 6,202,207 were, at the time the invention of the present application was made, commonly owned by International Business Machines Corporation.

Thus, US Patent 6,202,207 is disqualified as a reference in this 35 USC 103(a) rejection, pursuant to 35 U.S.C. 103(c). Therefore, the rejection of Claims 9-12, 26-29 and 31 under 35 U.S.C. § 103 has been overcome.

III.   Conclusion

It is respectfully urged that the subject application is patentable over the cited references and is now in condition for allowance. The Examiner is invited to call the undersigned at the below-listed telephone number if in the opinion of the Examiner such a telephone conference would expedite or aid the prosecution and examination of this application.

DATE: _6/15/05_

Respectfully submitted,
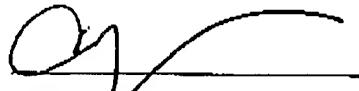
Cathrine K. Kinslow
Reg. No. 51,886
Wayne P. Bailey
Reg. No. 34,289
Yee & Associates, P.C.
P.O. Box 802333
Dallas, TX 75380
(972) 385-8777
Attorneys for Applicants

Page 13 of 13
Dawson, Jr. et al. – 09/692,988